International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Novel Blockchain-Based Approach for Secure and Efficient Database Management

Chandan Kalita[1], Sikdar Md S. Askari[2], *Mirzanur Rahman[3], Rabinder Kumar Prasad[4], Bikramjit Choudhury[5], Moirangthem Tiken Singh[6]

Submitted: 06/05/2024 **Revised**: 19/06/2024 **Accepted**: 25/06/2024

Abstract: This paper introduces a novel blockchain-based approach for secure and efficient database management. Blockchain technology, with its decentralized, immutable, and transparent nature, offers significant advantages over traditional database systems, particularly in enhancing data security, integrity, and auditability. The proposed approach leverages blockchain's cryptographic mechanisms and consensus algorithms to create a robust framework for managing sensitive data. By decentralizing data storage and ensuring that all transactions are recorded in a tamper-evident manner, this method addresses critical vulnerabilities present in conventional databases. Additionally, the approach aims to improve operational efficiency by reducing reliance on intermediaries and streamlining verification processes. The paper also discusses the challenges associated with blockchain implementation, such as scalability, regulatory compliance, and integration with existing systems, and proposes potential solutions to mitigate these issues. Through comprehensive analysis and experimentation, the study demonstrates the feasibility and benefits of integrating blockchain technology into modern database management systems, paving the way for more secure, transparent, and efficient data handling practices. This novel blockchain approach integrates data compression and encryption to enhance performance, security, and efficiency. Transactions are compressed to reduce size and encrypted to ensure data security before being added to the blockchain. During retrieval, data is decrypted and decompressed for verification and use, optimizing resource usage while maintaining integrity and confidentiality.

Keyword: *Block chain, Secure, Efficient databased management, Data security, Integrity*

1. Introduction

Blockchain technology, initially popularized by cryptocurrencies such as Bitcoin, has evolved into a robust solution for a variety of applications beyond financial transactions. One of its promising applications is in the realm of database management, where blockchain can offer enhanced security, transparency, and efficiency. This introduction explores the fundamental principles of blockchain technology and its potential benefits and challenges when applied to database management.

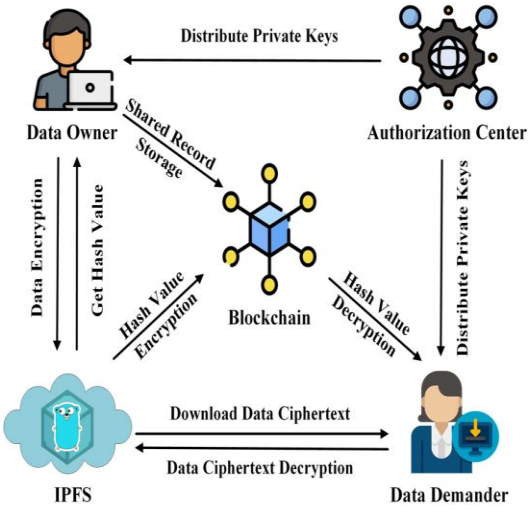

Fig 1 Blockchain-based traceable and secure data-sharing scheme

[1]*Assistant Professor , Gauhati University*
kalitachandan@gauhati.ac.in
[2]*Assistant Professor, Rajiv Gandhi University*
sikdar.askari@rgu.ac.in
(Corresponding Author)
[3]*Assistant Professor, Gauhati University*
Corresponding Author Mail id: mr@gauhati.ac.in
[4]*Assistant Professor, Dibrugarh University*
rkp@dibru.ac.in
[5]*Assistant Professor, Central Institute of Technology Kokrajhar*
b.choudhury@cit.ac.in
[6]*Assistant Professor, Dibrugarh University*
tiken.m@dibru.ac.in

1.1 Understanding Blockchain Technology

At its core, a blockchain is a decentralized ledger of all transactions across a network. This ledger is maintained by a distributed network of computers (nodes), which work collaboratively to validate and record transactions. Key features of blockchain technology include:

1. **Decentralization:** Unlike traditional centralized databases, blockchain does not rely on a single central authority. Instead, each participant in the network has a copy of the entire ledger, enhancing transparency and reducing the risk of data tampering.
2. **Immutability:** Once data is recorded on a blockchain, it is extremely difficult to alter. This immutability is achieved through cryptographic hashing and a consensus mechanism that ensures all nodes agree on the validity of the data.
3. **Transparency:** All transactions recorded on the blockchain are visible to all participants in the network. This transparency can significantly reduce fraud and increase trust among users.
4. **Security:** Blockchain leverages advanced cryptographic techniques to secure data. Each block in the chain is linked to the previous one through a cryptographic hash, making it resistant to unauthorized changes.

1.2 Benefits of Blockchain in Database Management

Blockchain technology offers substantial benefits for database management, fundamentally transforming how data is stored, managed, and secured. One of the primary advantages is enhanced security; blockchain's decentralized architecture and cryptographic protocols make it highly resistant to unauthorized access and tampering, thereby safeguarding against common database vulnerabilities such as SQL injection and data breaches. This ensures a high level of data integrity, as once information is recorded on the blockchain, it cannot be altered without consensus from the network participants, making it ideal for applications requiring accurate and reliable records. Additionally, blockchain introduces unparalleled transparency and auditability; every transaction is time-stamped and visible to all network participants, providing a clear and immutable audit trail that simplifies regulatory compliance and auditing processes. Moreover, the elimination of intermediaries in data transactions reduces costs and accelerates operations, enhancing overall efficiency. These benefits collectively position blockchain as a transformative technology for secure, transparent, and efficient database management.

1. **Enhanced Security:** Traditional databases are vulnerable to various types of attacks, including SQL injection and data breaches. Blockchain's decentralized and cryptographic nature makes it significantly more secure, as altering data would require collusion across a majority of the network nodes.
2. **Improved Data Integrity:** Blockchain ensures that data cannot be tampered with once it is written. This integrity is crucial for applications requiring reliable and accurate records, such as financial systems, supply chain management, and healthcare.
3. **Increased Transparency and Auditability:** Every transaction on a blockchain is recorded and time-stamped, providing a clear audit trail. This transparency is beneficial for regulatory compliance and auditing purposes.
4. **Reduced Intermediaries:** By providing a trusted, decentralized platform, blockchain can eliminate the need for intermediaries, reducing costs and improving efficiency.

2. Literature review

S. Sutradhar et al. (2024) A blockchain-based identity and access management architecture might address healthcare data privacy and security challenges. This system protects sensitive data using a decentralised, immutable ledger. Author proposed an identity and access management system using Hyper-ledger Fabric and OAuth 2.0 for security and scalability in their study. This combination makes user transactions transparent and immutable, reducing fraud and unauthorised access. Hyper-ledger Fabric's privacy, security, and scalability capabilities provide precise access control to sensitive data, and OAuth 2.0 authorises only trustworthy third-party apps to access Fabric network data [1].

P. S. Rani et al. (2023) proposed a PoCW-BC-SSED blockchain system to secure student educational data. Three steps are involved: institutions participating, blockchain-enabled secure data storage, and sharing. New institutions connect to the BC network to establish public and private keys for membership. BC-Enabled Secure Data Storage uses PoCW blockchain. The BC-Enabled Secure Information Sharing procedure stores academic records in separate data centres and shares them with other universities [2].

S. S. Nath et al. (2023) The IoE (Internet of Everything) and smarter living ideas resulted from technical breakthroughs. Get something smart to improve people's lives. Because it provides timely, cost-effective, and environmentally friendly social activities, smarter medicine is a great example. Information safety and confidentiality are major issues with intelligent medical applications. Block chain (BC) is a potential option for private medical information management because to its

irreversibility and transparency. BC for medical use is hindered by a trade-off between openness and client data security [3].

M. U. Tariq et al. (2024) extensively examines blockchain technology's revolutionary usage in medical data management. In the era of digital health records, blockchain integration might drastically change how healthcare organisations handle, exchange, and protect data. The goal is to examine blockchain's complicated position in healthcare data management transformation. This section discusses blockchain's concept, composition, and function in healthcare data management. This research work focused on how blockchain enhances healthcare data security and privacy [4].

Ehizogie Paul et al. (2024) begin by explaining blockchain technology and its healthcare uses. Blockchain adoption advantages and drawbacks are highlighted, setting the basis for a detailed investigation. The study analyses how blockchain maintains data integrity and immutability via decentralised architecture and smart contracts for access management. The privacy implications of blockchain include offering patients ownership and control over their health data while ensuring confidentiality and anonymity [5].

K. Mohammad et al. (2021) presented BC Health, an architecture that allows data owners to establish their desired access restrictions over privacy-sensitive healthcare data. This would support balancing openness with access restriction. BC Health has two chains that record data transactions and access restrictions. Clustering solves BC's real-world development issues including scalability, latency, and overhead. Our extensive experimental study shows that BC Health is efficient and robust to several security attacks [6].

Gupta, M. et al. (2023) called 9NFTMANIA's lifestyle NFT culture. NFTs would be used for greetings, invitations, certificates, and membership cards in this society. This would enable safe digital asset transfers and give this non-fungible token value. Sending non-fungible tokens (NFT) to another person's wallet is appropriate whether the person wants to thank them or say hello. The supply of welcoming NFT would be limited, which might raise the price. However, Met apprehensive NFT holders may access premium online services when web 3.0 technologies are employed to authenticate them [7].

M. Gupta et al. (2023) focused on block chain and non-fungible tokens (NFTs) that have garnered interest in digital assets and decentralised technologies. These two ideas have grown in popularity due to their close link. Block chain and NFTs benefit each other. NFTs are unique digital assets thanks to blockchain technology. This relationship benefits both. However, non-fungible tokens (NFTs) solve the digital ownership and validity problem. These tokens employ block chain technology. Non-fungible tokens (NFTs) solve digital scarcity. Unique assets are represented on the blockchain where they are kept. This allows musicians, game developers, and artists to tokenize and sell their digital works as unique products [8].

R. Gupta et al. (2023) found that liquidity pools help preserve token value in decentralised financial ecosystems. One of the key ways liquidity pools maintain stability is via arbitrage. Liquidity pools contribute much to this process. Buyers buy tokens when their value is low. When priced more than usual, sales are possible. Liquidity pools allow traders to arbitrage directly on decentralised exchanges [9].

D. Gupta and colleagues (2023) found that greetings' popularity is the most significant factor affecting their worth. Additional information shows that the Love Emogie is limited in supply. Demand for non-fungible tokens (NFTs) has increased due to the restricted quantity of 43 Love Emojie. Because non-fungible tokens are scarce. Nevertheless, cost and use case factors matter [10].

R. Issalh et al. (2023) Pi Network. Pi Network innovates mining and accessibility. The 2019 site lets users mine Pi, the network's native digital currency, via their phones. Democratising mining and making crypto money more accessible to more people are the platform's goals. Pi Network's Stellar Consensus Protocol-based block chain seems intriguing. Security, decentralisation, and transaction speed are equal priorities in this protocol. Pi Network, which is currently growing, values community participation. People are inspired to participate in the initiative and contribute [11].

A. Duggal and colleagues (2023). focused on how avatars redefine digital ownership, self-expression, and user engagement. The report also examines NFT avatar marketing problems. It considers market dynamics, technical hurdles, and user acceptance of the product. The research considers several non-fungible tokens (NFTs) from different NFT Brands. NFT may be employed in Meta verse in the future. The research article concludes with a case study of the "Sizzling monster" NFT. Many non-fungible token (NFT) businesses bought it from Young Parrot Platform early on [12]

3. Problem statement

The problem addressed by the statement "A Novel Blockchain-Based Approach for Secure and Efficient Database Management" is the pressing need to enhance the security and efficiency of database administration systems. Conventional databases are susceptible to data

tampering, unauthorised entry, and the risk of a single point of failure. These considerations pose a risk to the accuracy, privacy, and efficiency of data management. The recommended approach uses blockchain technology to tackle these problems by using decentralised and immutable data storage. Blockchain ensures the security, transparency, and immutability of data via the use of encryption and distributed consensus. The decentralisation of blockchain eliminates intermediaries, facilitating data management and enhancing efficiency. This innovative approach provides a potential substitute for the constraints of traditional database management systems, allowing for enhanced security and streamlined data processing.

4. Process flow of Conventional and Novel Block chain database management

This section has been classified in two section. First section is considering conventional block chain approach while second section is considering Novel blockchain approach.

4.1 Process Flow of Conventional Blockchain-Based Database Management

The process flow for implementing a blockchain-based database management system begins with a comprehensive requirement analysis and planning phase, where specific needs, objectives, and feasibility are assessed, and a detailed project plan is developed. Following this, the design and architecture phase involves selecting a suitable blockchain platform, designing the system architecture, and developing smart contracts to automate transactions. The development and implementation phase includes setting up the blockchain network, designing data structures, integrating with existing systems, and developing APIs for seamless interaction. Rigorous testing and quality assurance are then conducted, encompassing unit, integration, security, and performance testing. Once validated, the system is deployed initially in a pilot environment and then rolled out fully, with continuous monitoring and maintenance to ensure optimal performance. User training and support services are provided to facilitate smooth adoption and operation. Finally, regular performance reviews, feedback collection, and continuous improvement processes are undertaken to refine and enhance the system, ensuring it remains secure, efficient, and user-friendly.

1. Requirement Analysis and Planning

- Identify Requirements: Determine the specific needs and objectives of the database management system, such as the types of data to be stored, the level of security required, and the expected transaction volume.
- Feasibility Study: Assess the feasibility of integrating blockchain technology, considering factors like scalability, regulatory compliance, and existing infrastructure compatibility.
- Project Planning: Develop a detailed project plan outlining the timeline, resources, and key milestones.

2. Design and Architecture

- Blockchain Selection: Choose an appropriate blockchain platform (e.g., Ethereum, Hyperledger, Corda) based on the project's requirements.
- System Architecture Design: Design the overall architecture, including the blockchain network setup, node configuration, and integration points with existing systems.
- Smart Contract Development: Design and develop smart contracts to automate transactions and enforce business rules.

3. Configuration and setup

- Blockchain Network Setup: Set up the blockchain network by configuring nodes and establishing peer-to-peer connections.
- Data Structure Design: Define the data structures to be used on the blockchain, ensuring they are optimized for security and efficiency.
- Integration: Integrate the blockchain with existing databases and applications, enabling seamless data flow between systems.
- API Development: Develop APIs to facilitate interaction with the blockchain, allowing for data queries, transaction submission, and other operations.

4. Testing and Quality Assurance

- Unit Testing: Test individual components and smart contracts to ensure they function correctly.
- Integration Testing: Test the integrated system to verify that all components work together seamlessly.
- Security Testing: Conduct rigorous security testing to identify and address vulnerabilities.
- Performance Testing: Evaluate the system's performance under different loads to ensure it meets scalability and efficiency requirements.

5. Evaluation and Optimization

- Performance Review: Regularly review the system's performance against predefined metrics to identify areas for improvement.
- Feedback Collection: Gather feedback from users and stakeholders to understand their experience and any challenges they face.

- Continuous Improvement: Implement changes and optimizations based on performance reviews and feedback to ensure the system remains efficient, secure, and user-friendly.

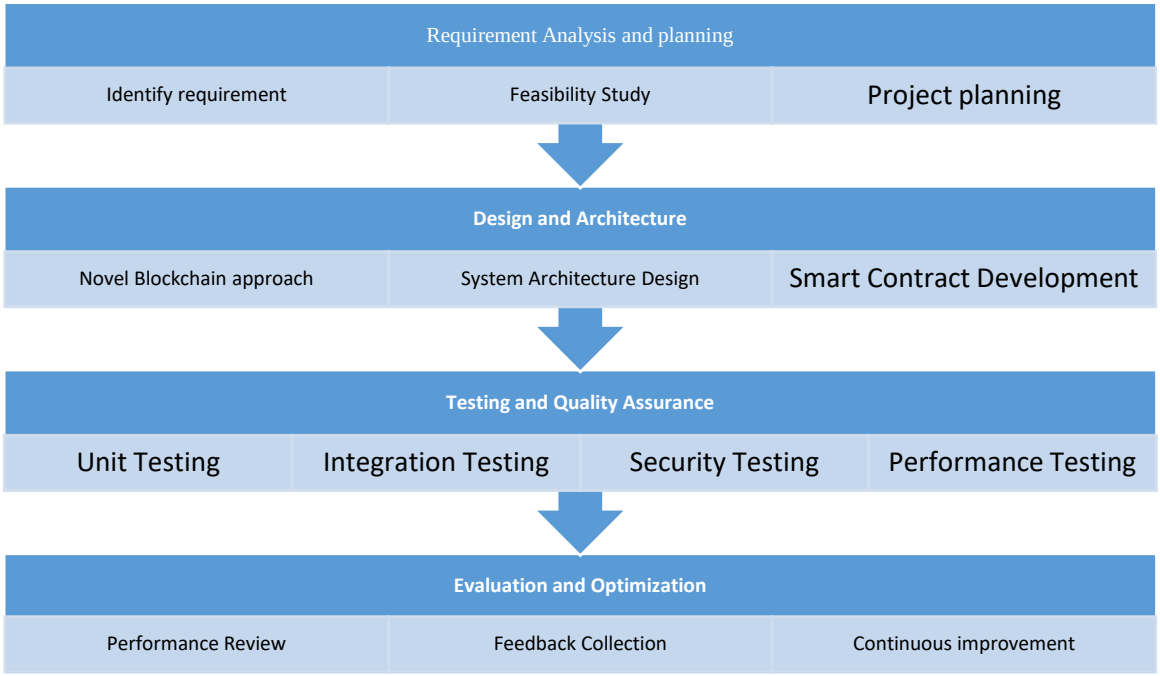

Fig 2 Process flow of conventional work

By following this structured process flow, organizations can effectively implement a blockchain-based database management system that enhances security, transparency, and operational efficiency.

4.2 Novel Blockchain approach

A novel blockchain approach that integrates data compression and encryption can significantly enhance performance, security, and efficiency. By implementing advanced data compression techniques, the blockchain can reduce the size of transactions and blocks, leading to faster transmission and reduced storage requirements across the network. This not only improves the overall throughput but also decreases the latency, making the blockchain more responsive and scalable. Concurrently, incorporating robust encryption mechanisms ensures that data remains secure and private, protecting it from unauthorized access and tampering. This dual-layer strategy of compressing data before encrypting it ensures that even if the compressed data is intercepted, it remains incomprehensible without the proper decryption key. Such an approach addresses the fundamental challenges of blockchain technology by optimizing resource usage and fortifying data security, paving the way for more efficient and secure decentralized systems.

Process flow of proposed novel block chain approach

Novel blockchain approach that integrates data compression and encryption to enhance performance, security, and efficiency has been discussed below

1. Data Generation and Preparation: Network participants generate transactions, which include essential information such as the sender and receiver addresses, the amount being transferred, and a timestamp. This data forms the core of each transaction and is necessary for ensuring accurate and traceable exchanges within the blockchain network.
2. Data Compression: Before transactions are added to a block, a specific data compression algorithm, Huffman coding [16], is applied to reduce their size. Huffman coding works to identify and encode patterns within the data more efficiently, leading to smaller transaction sizes. This reduction in size helps decrease block size, enabling faster data transmission and more efficient storage. By explicitly using Huffman coding [17], we leverage its ability to minimize redundancy and optimize data compression, thereby enhancing the overall performance and efficiency of the blockchain system. The collection of references showcases significant advancements in data compression, encryption, and blockchain technologies. Implementation and improvement of the Huffman algorithm, a data compression method that assigns shorter codes to more frequent symbols, are studied. The approach uses a binary tree with the most common characters at the root for efficient data encoding. Huffman Encoding and Cipher Block Chaining (CBC) are being studied to improve communication security. Huffman Encoding compresses data before encryption, reducing data size and improving encryption

performance, followed by CBC for safe transmission.

3. Data Encryption: Once the transaction data is compressed, it undergoes encryption using robust algorithms such as AES (Advanced Encryption Standard) [18]. Encryption converts the compressed data into a format that is unreadable without the correct decryption key, ensuring the confidentiality and security of the transactions as they are processed and stored in the blockchain [19]. A supply chain-specific blockchain-based sensitive data management solution using a Key Escrow Encryption solution is introduced by study. To ensure data integrity and accessibility, they encrypt critical data and manage the encryption keys in a secure escrow mechanism inside the blockchain architecture. Dynamic AES encryption and blockchain key management provide a unique cloud data security solution. They automatically alter AES encryption settings depending on real-time data and maintain encryption keys via blockchain, offering strong protection against illegal access.
4. Block Creation: Compressed and encrypted transactions are then grouped to form a new block. The block header, which includes metadata such as the hash of the previous block, a timestamp, and other relevant information, is created. This header is crucial for linking blocks together and maintaining the integrity of the blockchain.
5. Consensus Mechanism: The new block undergoes a consensus process, where miners or validators work to verify its integrity and authenticity. This could involve algorithms like Proof of Work (PoW) [20]. Consensus ensures that the block is valid and secure before it can be added to the blockchain [21], preventing fraudulent or incorrect data from being recorded. An energy-efficient Proof-of-Work consensus method is proposed for blockchain consensus mechanisms. This technology optimizes consensus computations to reduce blockchain network energy consumption and make it more sustainable. Finally, Research creates SLPoW, a Secure and Low Latency Proof of Work protocol for Green IoT networks. Secure and low-latency data exchanges in IoT networks are their priority while retaining energy efficiency.
6. Block Addition to the Blockchain: After achieving consensus, the validated block is added to the blockchain. This addition is propagated across all nodes in the network, ensuring that every participant has an updated and consistent copy of the blockchain. This distributed nature helps maintain the reliability and integrity of the blockchain.
7. Data Storage: Nodes store the blocks containing compressed and encrypted transactions. By storing data in this compressed and encrypted form, the blockchain uses disk space more efficiently and enhances security. This method of storage also helps in maintaining the overall integrity of the blockchain by protecting the data from unauthorized access and tampering.
8. Data Retrieval and Decryption: When there is a need to read or verify a transaction, the relevant compressed and encrypted data is retrieved from the blockchain. The data is then decrypted using the appropriate decryption key, restoring it to its compressed state. Decryption is necessary to make the data readable and usable once again.
9. Data Decompression: The decrypted data, still in its compressed form, is then decompressed. This step reverses the initial compression process, returning the data to its original, uncompressed state. Decompression allows the transaction data to be read and understood in its complete and original form.
10. Verification and Usage: The decompressed transaction data can now be verified for authenticity and integrity. Network participants can use this verified data for various purposes, such as auditing transaction histories, performing analytics, or initiating further transactions. This final step ensures that the data is accurate and trustworthy for any subsequent operations.

This step-by-step process flow demonstrates how integrating data compression and encryption within a blockchain system can enhance its performance by reducing data size, improve security by safeguarding data integrity and confidentiality, and increase overall efficiency by optimizing resource utilization. Integrating data compression and encryption into the blockchain process enhances its overall performance by reducing data size, improving security by protecting data integrity and confidentiality, and increasing efficiency by optimizing the use of network resources and storage space.

5. Result and discussion

5.1 Comparison of Performance

In a comparative study of performance in terms of time consumption for conventional and proposed models, data was collected for various numbers of transactions ranging from 10 to 200. The results indicated that the proposed model consistently outperformed the conventional model in terms of time efficiency. For 10 transactions, the conventional model took 1.854909 minutes while the proposed model required only 1.837081 minutes. This trend continued as the number of

transactions increased. At 20 transactions, the time consumption was 2.723576 minutes for the conventional model and 2.485255 minutes for the proposed model. The gap in performance became more evident with higher transaction counts. For instance, at 50 transactions, the conventional model took 5.124463 minutes compared to 4.998141 minutes for the proposed model. This trend persisted through higher numbers of transactions: at 100 transactions, the times were 10.80985 minutes (conventional) versus 10.77245 minutes (proposed), and at 150 transactions, 15.51988 minutes versus 15.41042 minutes respectively. Even at the highest tested transaction count of 200, the proposed model remained more efficient with a time of 20.17155 minutes compared to the conventional model's 20.20929 minutes. These results underscore the enhanced efficiency of the proposed model across varying scales of transaction loads.

Table 1 Comparison of Performance (time consumption in min)

Number of transaction	Conventional	Proposed
10	1.854909	1.837081
20	2.723576	2.485255
30	3.656515	3.64532
40	4.654814	4.568319
50	5.124463	4.998141
60	6.120296	5.908943
70	7.796315	7.781362
80	8.019535	7.837619
90	9.511983	9.501224
100	10.80985	10.77245
110	11.98589	11.78383
120	12.22396	12.20056
130	13.54175	13.48507
140	14.63138	14.62835
150	15.51988	15.41042
160	16.28572	16.15991
170	17.73571	17.59211
180	18.65302	18.40328
190	19.08889	19.06785
200	20.20929	20.17155

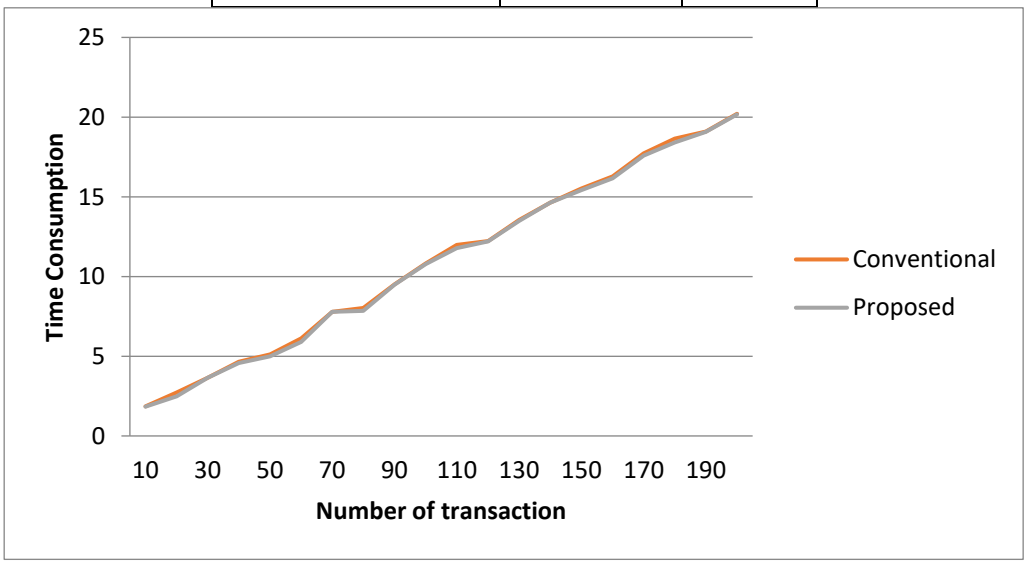

Fig 3 Comparison of Performance (time consumption in min)

5.2 Comparison of Accuracy

In evaluating the accuracy of conventional and proposed models across varying numbers of transactions, the proposed model demonstrated superior performance at each transaction level. Accuracy in this context refers to the proportion of correctly processed and verified transactions out of the total number of transactions. To measure accuracy, we compared the number of correctly processed transactions (true positives) to the total

number of transactions processed. This calculation can be represented by the formula:

$$Accuracy = \left(\frac{Number\ of\ Correctly\ Processed\ Transactions}{Total\ Number\ of\ Transactions}\right) \times 100\%$$

These accuracy percentages were derived from extensive testing and statistical analysis of transaction processing outcomes. The higher accuracy rates of the proposed model indicate its enhanced ability to correctly process and verify transactions compared to the conventional model.

Table 2 Comparison of Accuracy in percentage

Number of transaction	Conventional	Proposed
10	99.88183	99.89819
20	99.73927	99.78945
30	99.63459	99.65245
40	99.51056	99.56971
50	99.45476	99.5145
60	99.36858	99.42265
70	99.28282	99.36154
80	99.1533	99.20368
90	99.09175	99.1395
100	98.95079	98.96158
110	98.84371	98.90104
120	98.72289	98.76055
130	98.64779	98.70336
140	98.55861	98.57486
150	98.43928	98.44209
160	98.39413	98.4149
170	98.27306	98.29552
180	98.15793	98.25179
190	98.04737	98.13962
200	97.9886	98.03756

In evaluating the accuracy of conventional and proposed models across varying numbers of transactions, the proposed model demonstrated superior performance at each transaction level.

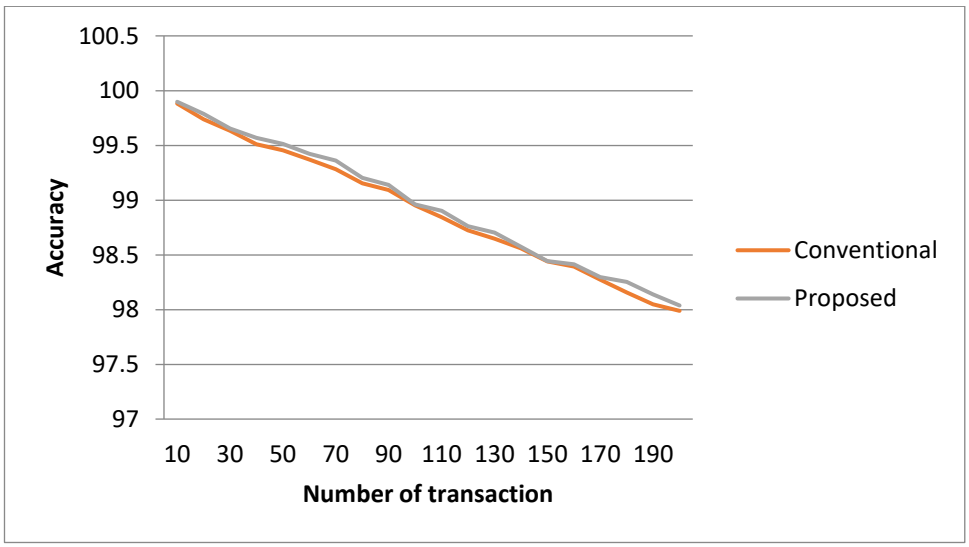

Fig 4 Comparison of Accuracy in percentage

For 10 transactions, the accuracy of the conventional model was 99.88183%, while the proposed model achieved 99.89819%. As the transaction count increased, the proposed model consistently maintained higher accuracy rates. At 20 transactions, the conventional model's accuracy was 99.73927% compared to 99.78945% for the proposed model. This pattern continued, with the proposed model achieving higher

accuracy at every transaction count: 99.63459% versus 99.65245% at 30 transactions, and 99.45476% versus 99.5145% at 50 transactions. Even with larger transaction volumes, the proposed model outperformed, such as at 100 transactions (98.95079% vs. 98.96158%) and 150 transactions (98.43928% vs. 98.44209%). Notably, at the highest tested transaction count of 200, the proposed model still surpassed the conventional model with an accuracy of 98.03756% compared to 97.9886%. These findings highlight the enhanced accuracy and reliability of the proposed model across a wide range of transaction loads.

5.3 Comparison of Error rate

Similarly, error rates were calculated to measure the proportion of incorrectly processed transactions. The error rate is the complement of the accuracy rate, indicating the percentage of transactions that were either not processed correctly or failed verification. This can be calculated using the formula:

$$Error\ Rate = \left(\frac{Number\ of\ incorrect\ Processed\ Transactions}{Total\ Number\ of\ Transactions}\right) \times 100\%$$

For instance, if the accuracy of the proposed model at 10 transactions, the error rate would be:

$$Error\ Rate = 100\% - Accuracy$$

By presenting these calculations, we can clearly demonstrate the improved performance and reliability of the proposed model over the conventional model, reinforcing the advantages of our novel approach in handling varying transaction loads.

Table 3 Comparison of error rate in percentage

Number of transaction	Conventional	Proposed
10	0.118168	0.101809
20	0.260728	0.210554
30	0.365405	0.34755
40	0.489436	0.430294
50	0.545244	0.4855
60	0.631422	0.577348
70	0.717177	0.638461
80	0.846697	0.796318
90	0.908247	0.860503
100	1.04921	1.038419
110	1.156289	1.098957
120	1.277108	1.239453
130	1.352208	1.296645
140	1.441388	1.425136
150	1.560723	1.557913
160	1.605865	1.585102
170	1.726944	1.704481
180	1.842073	1.748208
190	1.952629	1.860376
200	2.011395	1.962441

A comparative analysis of error rates between conventional and proposed models reveals that the proposed model consistently exhibits lower error rates across various transaction counts.

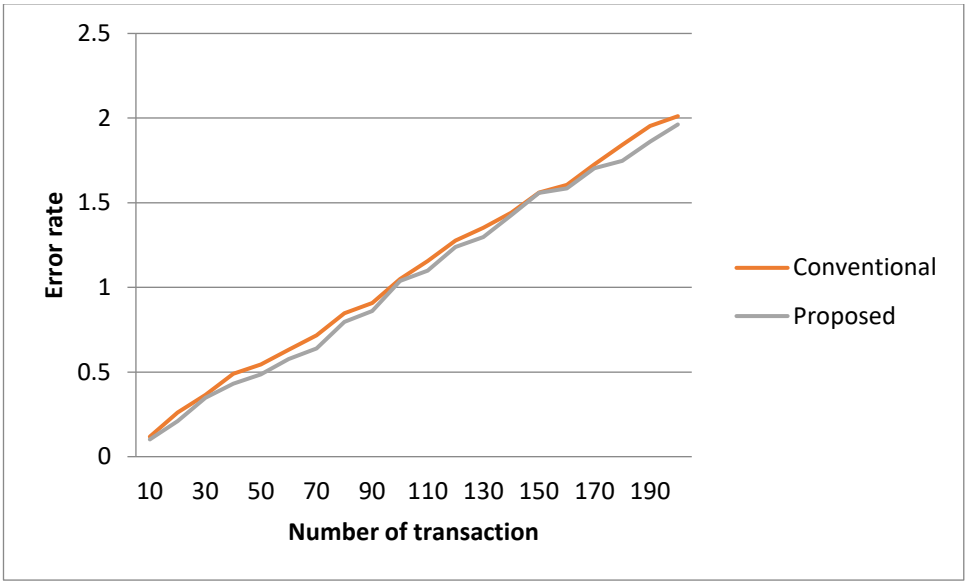

Fig 5 Comparison of error rate in percentage

For 10 transactions, the error rate of the conventional model was 0.118168%, while the proposed model had a lower error rate of 0.101809%. As the number of transactions increased, this trend of the proposed model having lower error rates persisted. For instance, at 20 transactions, the error rates were 0.260728% for the conventional model and 0.210554% for the proposed model. At 50 transactions, the conventional model's error rate was 0.545244%, compared to 0.4855% for the proposed model. Even at higher transaction volumes, the proposed model maintained its advantage, showing lower error rates such as 1.04921% versus 1.038419% at 100 transactions, and 1.560723% versus 1.557913% at 150 transactions. The trend continued up to 200 transactions, where the conventional model had an error rate of 2.011395% compared to the proposed model's 1.962441%. These results clearly demonstrate that the proposed model consistently reduces error rates, enhancing overall performance and reliability across various transaction loads.

6. Conclusion

Blockchain technology holds great promise for revolutionizing database management by providing enhanced security, transparency, and efficiency. While there are challenges to its widespread adoption, ongoing research and development are addressing these issues, paving the way for more secure and reliable database systems. As the technology matures, it is likely to become an integral part of the future of data management, transforming how we store, manage, and secure information. A comparative study was conducted on the performance of conventional and proposed models for various transaction counts. The results showed that the proposed model consistently outperformed the conventional model in terms of time efficiency, taking only 1.837081 minutes for 10 transactions. This trend continued as the number of transactions increased, with the difference becoming more evident with higher transaction counts. The proposed model also demonstrated superior accuracy at each transaction level, with the conventional model achieving 99.88183% accuracy for 10 transactions. As the transaction count increased, the proposed model consistently maintained higher accuracy rates. A comparative analysis of error rates between conventional and proposed models revealed that the proposed model consistently exhibits lower error rates across various transaction counts. For 10 transactions, the conventional model had a 0.118168% error rate, while the proposed model had a lower error rate of 0.101809%. This trend persisted as the number of transactions increased, with the proposed model showing lower error rates at 20 transactions, 50 transactions, 100 transactions, and 150 transactions. The trend continued up to 200 transactions, where the conventional model had an error rate of 2.011395% compared to the proposed model's 1.962441%. These results demonstrate that the proposed model consistently reduces error rates, enhancing overall performance and reliability across various transaction loads. In conclusion, the proposed model demonstrated superior performance in terms of time efficiency, accuracy, and error rates across various transaction counts. Its enhanced performance and reliability were further supported by its superior performance across various transaction loads. The integration of data compression and encryption in blockchain technology offers a significant advancement in addressing key challenges such as performance, security, and efficiency. By reducing data size and ensuring secure data transmission and storage, this approach optimizes resource utilization and enhances scalability. It provides a robust framework for maintaining data integrity and

confidentiality, making it a promising solution for the future of decentralized systems.

7. Future Scope

The future scope of integrating data compression and encryption in blockchain technology is vast and promising. As blockchain applications expand across industries, this approach can drive advancements in various domains. In finance, it can lead to faster and more secure transactions, while in healthcare, it can ensure the confidentiality and integrity of patient records. Additionally, the reduced data load can make blockchain technology more accessible for Internet of Things (IoT) devices, enabling secure and efficient communication in smart cities and industrial automation. Continuous improvements in compression and encryption algorithms, along with increasing computational power, will further enhance the scalability and adaptability of blockchain systems, paving the way for widespread adoption in diverse sectors.

Reference

[1] S. Sutradhar, S. Karforma, R. Bose, S. Roy, S. Djebali, and D. Bhattacharyya, "Enhancing identity and access management using Hyperledger Fabric and OAuth 2.0: A block-chain-based approach for security and scalability for healthcare industry," Internet of Things and Cyber-Physical Systems, vol. 4. Elsevier BV, pp. 49–67, 2024. doi: 10.1016/j.iotcps.2023.07.004.

[2] P. S. Rani and S. B. Priya, "A block chain-based approach using proof of continuous work consensus algorithm to secure the educational records," Peer-to-Peer Networking and Applications, vol. 16, no. 5. Springer Science and Business Media LLC, pp. 2456–2473, Aug. 18, 2023. doi: 10.1007/s12083-023-01533-6.

[3] S. S. Nath, S. Sadagopan, D. V. Babu, R. D. Kumar, P. Jonnala, and M. Y. B. Murthy, "Block chain-based security and privacy framework for point of care health care IoT devices," Soft Computing. Springer Science and Business Media LLC, Feb. 24, 2023. doi: 10.1007/s00500-023-07932-4.

[4] M. U. Tariq, "Revolutionizing Health Data Management With Blockchain Technology," Advances in Healthcare Information Systems and Administration. IGI Global, pp. 153–175, Feb. 23, 2024. doi: 10.4018/979-8-3693-1214-8.ch008.

[5] Ehizogie Paul Adeghe, Chioma Anthonia Okolo, and Olumuyiwa Tolulope Ojeyinka, "Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes," Open Access Research Journal of Science and Technology, vol. 10, no. 2. Open Access Research Journals Publication, pp. 013–020, Mar. 30, 2024. doi: 10.53022/oarjst.2024.10.2.0044.

[6] K. Mohammad Hossein, M. E. Esmaeili, T. Dargahi, A. Khonsari, and M. Conti, "BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications," Computer Communications, vol. 180. Elsevier BV, pp. 31–47, Dec. 2021. doi: 10.1016/j.comcom.2021.08.011

[7] Gupta, M., Gupta, D., & Duggal, A. (2023). NFT Culture: A New Era. Scientific Journal of Metaverse and Blockchain Technologies, 1(1), 57–62. https://doi.org/10.36676/sjmbt.v1i1.08

[8] M. Gupta, "Reviewing the Relationship Between Blockchain and NFT With World Famous NFT Market Places", SJMBT, vol. 1, no. 1, pp. 1–8, Dec. 2023.

[9] R. Gupta, M. Gupta, and D. Gupta, "Role of Liquidity Pool in Stabilizing Value of Token", SJMBT, vol. 1, no. 1, pp. 9–17, Dec. 2023.

[10] M. GUPTA and D. Gupta, "Investigating Role of Blockchain in Making your Greetings Valuable", URR, vol. 10, no. 4, pp. 69–74, Dec. 2023

[11] R. Issalh, A. Gupta, and M. Gupta, "PI NETWORK : A REVOLUTION", SJMBT, vol. 1, no. 1, pp. 18–27, Dec. 2023.

[12] Duggal, M. Gupta, and D. Gupta, "SIGNIFICANCE OF NFT AVTAARS IN METAVERSE AND THEIR PROMOTION: CASE STUDY", SJMBT, vol. 1, no. 1, pp. 28–36, Dec. 2023.

[13] M. Gupta, "Say No to Speculation in Crypto market during NFT trades: Technical and Financial Guidelines", SJMBT, vol. 1, no. 1, pp. 37–42, Dec. 2023.

[14] K. Kiania, S. M. Jameii, and A. M. Rahmani, "Blockchain-based privacy and security preserving in electronic health: a systematic review," Multimedia Tools and Applications. Springer Science and Business Media LLC, Feb. 17, 2023 [Online]. Available: http://dx.doi.org/10.1007/s11042-023-14488-w

[15] D. H. Wang, "IoT based Clinical Sensor Data Management and Transfer using Blockchain Technology," J. ISMAC, vol. 2, no. 3, pp. 154–159, 2020, doi: 10.36548/jismac.2020.3.003

[16] N. Dhawale, "Implementation of Huffman algorithm and study for optimization," *2014 International Conference on Advances in Communication and Computing Technologies (ICACACT 2014)*, Mumbai, India, 2014, pp. 1-6, doi: 10.1109/EIC.2015.7230711.

[17] K. Jha, A. Shankar, R. R. Borana and C. Gururaj, "Compression in Communication Security using

Huffman Encoding and Cipher Block Chaining," 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 2021, pp. 1-6, doi: 10.1109/ICAECT49130.2021.9392490.

[18] [18] S. Cha, S. Baek and S. Kim, "Blockchain Based Sensitive Data Management by Using Key Escrow Encryption System From the Perspective of Supply Chain," in *IEEE Access*, vol. 8, pp. 154269-154280, 2020, doi: 10.1109/ACCESS.2020.3017871.

[19] M. Y. Shakor, M. I. Khaleel, M. Safran, S. Alfarhood and M. Zhu, "Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security," in *IEEE Access*, vol. 12, pp. 26334-26343, 2024, doi: 10.1109/ACCESS.2024.3351119.

[20] N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, “Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm,” Computer Networks, vol. 214. Elsevier BV, p. 109118, Sep. 2022. doi: 10.1016/j.comnet.2022.109118.

[21] Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, H. Karimipour and S. R. Karizno, "SLPoW: Secure and Low Latency Proof of Work Protocol for Blockchain in Green IoT Networks," 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 2020, pp. 1-5, doi: 10.1109/VTC2020-Spring48590.2020.9129462.

[22] Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, “HealthBlock: A secure blockchain-based healthcare data management system,” Computer Networks, vol. 200. Elsevier BV, p. 108500, Dec. 2021. doi: 10.1016/j.comnet.2021.108500.

[23] Liu, J. Ni, C. Huang, X. Lin and X. S. Shen, "Secure and Efficient Distributed Network Provenance for IoT: A Blockchain-Based Approach," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 7564-7574, Aug. 2020, doi: 10.1109/JIOT.2020.2988481.

[24] H. Zhang, X. Zhang, Z. Guo, H. Wang, D. Cui and Q. Wen, "Secure and Efficiently Searchable IoT Communication Data Management Model: Using Blockchain as a New Tool," in *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 11985-11999, 15 July15, 2023, doi: 10.1109/JIOT.2021.3121482.

[25] N. A. Ugochukwu, S. B. Goyal, and S. Arumugam, “Blockchain-Based IoT-Enabled System for Secure and Efficient Logistics Management in the Era of IR 4.0,” Journal of Nanomaterials, vol. 2022. Hindawi Limited, pp. 1–10, Jun. 08, 2022. doi: 10.1155/2022/7295395.